State of Colorado

2006 Information and Technology Strategic Plan

(2006-2009)

Revised February 2006

Commission on Information Management (IMC)

Governor's Office of Innovation and Technology (OIT)

STATE OF COLORADO

OFFICE OF INNOVATION AND TECHNOLOGY (OIT)
COMMISSION ON INFORMATION MANAGEMENT (IMC)
Office of the Governor
225 East 16th Avenue, Suite 260
Denver, Colorado 80203
Phone: 303-866-6060
FAX: 303-866-6454

February 20, 2006

Bill Owens
Governor

John Picanso
IMC Chairman
OIT Director
State Chief Information Officer

The 2006 Colorado State Information and Technology Strategic Plan presents an information technology plan for the State, independent of whom within state government is responsible for delivering a particular action item. The plan focuses on delivering four key initiatives, three of which will yield benefits in the current year. The fourth initiative implements a more collaborative process for the approval of Department IT Plans and other information technology requests, thus allowing departments the opportunity to better plan their information technology investments. This plan clearly describes each initiative and outlines the objectives, action items and the information technology or public service professional responsible for each action. This plan upholds the Governor's highest priority information technology commitments and aligns with the Governor's Office of Innovation and Technology's adopted mission.

This updated plan replaces both the 2004 Statewide Information Technology Plan and the 2004 Strategic Communications and Data Processing Plan. This enterprise plan will guide the acquisition, management, and use of technology across Colorado State government for the next four years (2006-2009).

The plan builds on the two most significant information technology accomplishments of 2005: the creation of the new Colorado Information Security Program and implementation of the Statewide Internet Portal through the formation of the Statewide Internet Portal Authority. The plan also builds on many other initiatives underway such as the significant work begun on e-mail consolidation, cyber-security policies and standards, state agency migration to the Statewide Internet Portal, and information technology contract management and project management best practices.

While we have made substantial improvement in a number of areas, much work remains to be done. The plan has an aggressive timetable for implementation. We are asking a great deal of ourselves, and we will need the strong support of the State's Executive, Legislative, and Judicial Branches to accomplish the objectives stated in this document. This plan is worthy of that support; it redefines how we manage our information technology resources. For the State's information technology leaders, that is our challenge, our obligation and our opportunity.

John Picanso
Chief Information Officer
State of Colorado

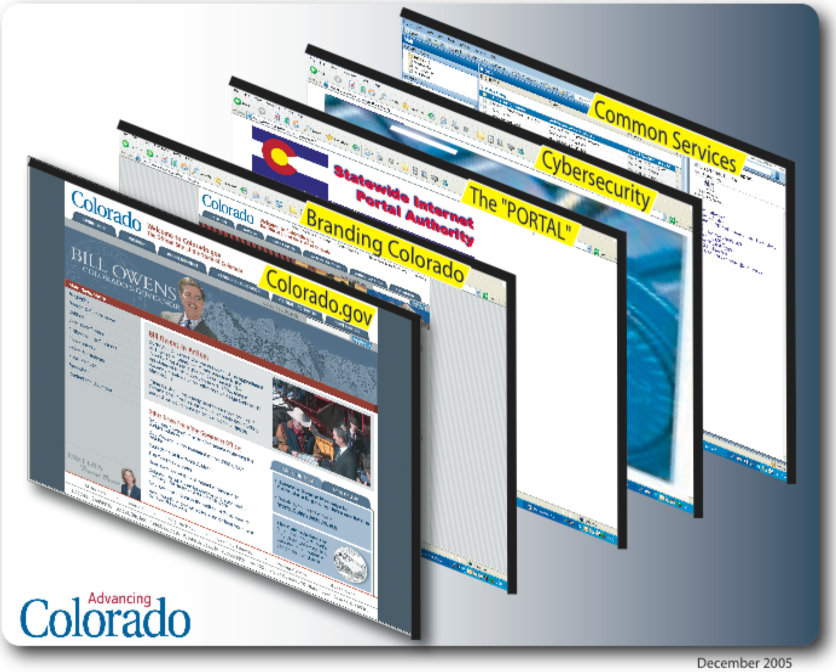
Table of Contents

Introduction

The 2006 Colorado State Information and Technology Strategic Plan outlines a bold but necessary agenda for redefining how we manage our information technology resources to improve service delivery and streamline business operations. Colorado State Government can maximize the value that its technology investment delivers to Colorado citizens and businesses by pursuing the four initiatives identified in this plan: improved security of our information, better integration and access to government services for our constituents, better application of the economies of scale to improve our use of capital, and further leveraging of our IT governance structure to oversee our strategic planning efforts.

The plan supports Branding Colorado and the Colorado.gov Website and upholds the Governor's highest information technology priority commitments, including The Portal, Cyber-Security, and Common Services. The interrelationship among Branding Colorado, the Colorado.gov Website, and the three information technology priorities is depicted below in Figure 1: Advancing the Enterprise Technology Portfolio.

Figure 1: Advancing the Enterprise Technology Portfolio



December 2005

The implementation of this plan will help to fulfill the Governor's Office of Innovation and Technology's adopted mission:

> *To increase the effectiveness of government through the use of shared information and technology. Information technology will be used to maximize the efficiency of service delivery and will operate as a seamless enterprise, delivering consistent, cost-effective, reliable, accessible and secure services that satisfy the needs of the citizens of Colorado, its business communities, and its public sector agencies.*

Not depicted in Figure 1, but equally important, is our governance structure. The Colorado Commission on Information Management (IMC) / Governance initiative will deliver an assessment model that will be used to evaluate annual Department IT Plans (DITPs), IT requests, IT project proposals, and IT Procurements. Communicating the assessment model to each department prior to their IT submissions will enhance their ability to better plan information technology investments and optimize the value those investments create for the entire state enterprise.

Although departments and programs each have some unique technology needs, most or all state programs and customers share many important needs that a statewide information technology strategic plan serves best. The statewide information technology strategic plan, therefore, can be a key contributor to the execution of state programs and the measure of their success.

A key focus of this plan is to align technology at the enterprise level and focus our investments on those initiatives that will enable significant statewide improvement.

The 2006 Colorado State Information and Technology Strategic Plan identifies four key initiatives on which to focus our efforts over the next four years:

Initiative 1: **Cyber-Security** - Improved security of information;

Initiative 2: **e-Government / Portal** - Better integration and access to government services;

Initiative 3: **Common / Shared Services** - Better application of economies of scale and improved use of; and,

Initiative 4: **IMC / Governance** – Further leveraging our information technology governance structure to assure continuity in planning and controlling the state's investment in information technology.

These initiatives and their associated objectives and action items, detail the steps necessary to maximize the value of our information technology, improve service delivery and streamline business operations.

The plan describes each initiative, identifies the key objectives within each initiative, and lists the actionable steps that will insure this plan becomes a reality. Action items are generally limited to the next 12-18 months in order to remain as concrete and meaningful as possible. Full implementation of an initiative or objective, therefore, may require additional action items that are not included in this document.

The 2006 Colorado State Information and Technology Plan identifies those across state government responsible for delivering to the Colorado State Government and all constituents the value of technology: a safe, integrated and accessible government information technology that uses capital efficiently and effectively. The Governor's Office of Innovation and Technology (OIT) will facilitate the delivery of the 2006 Colorado State Information and Technology Plan and the value it promises.

This page intentionally left blank

Initiatives, Objectives & Actions

Initiative 1: Cyber-Security

To ensure Colorado information technology infrastructure is secure and privacy is protected

Faced with increasing cyber attacks, more demanding regulatory compliance, reduced tolerance for service disruption and the rise of domestic and international terrorism, the state must deploy, coordinate and enforce an information security program that ensures the confidentiality, integrity and availability of our mission critical data as well as the privacy of our citizens. Securing cyberspace is a difficult strategic challenge that requires a coordinated and a focused statewide effort.

The State will develop and implement the Colorado Information Security Program (CISP) to institutionalize information security policies and controls statewide. The CISP will establish guidelines and provide direction to state public agencies on formal procedures for enhancing enterprise level information security and minimum compliance activities. The CISP will also guide the identification of the state’s most critical information technology assets and the performance of risk assessments of those systems critical systems. Finally, the CISP will establish a formal Colorado Incident Response Program and create a training system that meets the requirements of educating technical security professionals, state public agency employees, and Colorado citizens. For the later two, groups would receive primarily awareness training.

The following four objectives address each of the key elements within the CISP: strategic planning, tactical protection, incident response, and awareness training.

Cyber-Security Objective 1: The State will develop and implement the Statewide Colorado Information Security Program (CISP)

By defining a program with clear security standards, the CISP will establish an environment that provides measurable standards for risk mitigation and offer state agencies the tools necessary to secure their information technology operations. By addressing specific risks with proven security processes embedded in the standards, the State will provide a model for efficient and effective risk mitigation. The CISP will also provide users of state systems with a clear understanding of their obligations to protect state systems and data. In addition to the CISP, the State will complete the development and implementation of a comprehensive series of information security policies and supporting standards with central authority to enforce provisions of the CISP across all state agencies.

Actions to Achieve Cyber-Security Objective 1

1. By July 2006, the **Chief Information Security Officer (CISO)** will publish the Colorado Information Security Program (CISP) plan.
2. By July 2006, the **CISO** will publish a comprehensive series of policies that address all facets of information security in information technology operations.
3. By December 31, 2006 the **CISO** shall report to the Governor and State Legislature on the general state of information security within state public agencies.

Cyber-Security Objective 2: The state will identify the most critical information technology systems and assets and implement appropriate security measures to address and mitigate vulnerabilities

The State will conduct a comprehensive inventory of all state and department information technology systems and assets and prioritize these systems and assets in accordance with Federal Information Processing Standards (FIPS) Publication 199 criteria. FIPS Publication 199 defines three levels of *potential impact* on organizations should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). This inventory process will identify state government's most critical assets and the minimum information security requirements for these assets and will provide a measuring stick for determining the appropriate resources required to mitigate system or asset vulnerabilities.

Actions to Achieve Cyber-Security Objective 2

1. By June 2006, the **CISO** and **OIT**, in cooperation with state agency Chief Information Officers (CIOs), and the State's Continuity of Government (COG) Project Manager (CDOLA/DEM), will complete an inventory of critical state systems.
2. By July 2006, the **CISO**, in cooperation with the state agency CIOs, will identify and develop a *confidential,* prioritized list of critical State systems based upon FIPS 199 criteria.
3. By August 2006, the **CISO**, in cooperation with the state agency CIO's, will perform risk assessments of systems on the prioritized list.
4. By September 2006, **state agency CIOs** will provide a roadmap for identifying resources and requirements necessary to adequately secure their information technology systems and assets according to the FIPS 199 criteria.
5. By December 31, 2006, the **CISO** shall report to the Governor and Colorado General Assembly on the general state of information security for critical State systems.

Cyber-Security Objective 3: The State will establish the Colorado Incident Response Program and train a cadre of security professionals to respond appropriately to cyber-security incidents

The State will develop and implement the Colorado Incident Response Program. Judicious and proper identification of cyber-security incidents is critical to coordinating activities of state agencies experiencing similar or related attacks upon their data and network infrastructure. The ability to collect statewide information on the types of vulnerabilities that are being exploited, frequency of attacks, and costs of recovering from an attack are critical to an effective incident response program. The goal of the Colorado Incident Response Program is to ensure state agencies can recover from a cyber-security incident in a timely and secure manner and to minimize the impact on other state agencies.

Actions to Achieve Cyber-Security Objective 3

1. By June 30, 2006, the **CISO** will develop the Colorado Incident Response Program including goals, scope, roles and responsibilities, and procedures.
2. By July 31, 2006, the **CISO** will establish the Colorado Cyber Security website. This website will include links for Security Advisories and Incident Reporting.
3. By August 30, 2006, the **CISO** will establish the Computer Incident Response Team (CIRT) with members from all state agencies and provide CIRT training fundamentals.
4. By Dec 31, 2006, the **state agencies** will participate in a cyber-security exercise program to include department-level, regional-level, and state-level cyber-security exercises.

Cyber-Security Objective 4: The State will establish an Information Security Training program for security professionals from state agencies and a statewide Information Security Awareness program for state agency employees and Colorado citizens

The State will develop and implement a comprehensive information security training and awareness program to address pervasive ignorance of cyber-security threats and vulnerabilities. Due to the obscure and technical nature of information security, too many people are unaware of the many small tasks that can be accomplished to make our information technology environment more secure.

Actions to Achieve Cyber-Security Objective 4

1. By July 31, 2006, the **CISO** will develop Standard Operating Procedures (SOPs) for content and delivery of cyber security awareness training.
2. By August 31, 2006, the **CISO** will deploy a Web-based, centrally administered training system to provide cyber-security training to state agency employees and security professionals.
3. By December 31, 2006, the **CISO** will provide statistical information to the Governor and Colorado General Assembly on the level of security awareness training completed among state agency employees.

Initiative 2: e-Government / Portal

Use shared information and common technology across agencies to extend access to and streamline delivery of government services to constituents anywhere, anytime

e-Government (i.e., electronic government) has been a key initiative for at least the past ten years in Colorado State Government.

The key to the implementation of this initiative is the establishment of a robust statewide Internet portal that enables one-stop customer access to all government information and services. Whether individual citizens and businesses serve themselves (via the portal) or seek service from government staff (who access the portal on the constituents' behalf), the portal assists by maximizing the services available through the electronic channel. In this way the State can provide a consistent interface to users, that is easily recognizable, secure, and operationally efficient.

e-Government, including an Internet portal, is an integral component of any multi-channel strategy. The transactions conducted through the portal will include the retrieval of public information, the renewal of licenses or the registration of an entity to do business within the state.

e-Government / Portal Objective 1: The State will adopt a statewide Enterprise Architecture (EA)

The State will adopt an EA as a means of connecting individual agency goals to a shared information technology strategy thereby helping the enterprise improve the return on its information technology investments. To this end, the State will define shared processes and functions, the shared data needs of various users, technology standards, and reusable common services that can be availed by multiple systems. These business, information, application, and technology architectures will be communicated as reference models.

The EA will accelerate the improvement of both internal efficiency and external effectiveness by separating agency processes and services from the technologies that support them. Such a division permits modifying the fast-changing technologies independently from the slower-changing agency processes.

Actions to Achieve e-Government / Portal Objective 1

1. By June 30, 2006, the **IMC** will review all policies, standards, and guidelines and update those that require modification.
2. By June 1, 2006, **agencies** will submit their compliance to the IMC policies and standards as part of their annual DITP.
3. By December 15, 2006, the **IMC** and **OIT** will develop initial versions of the following EA deliverables:
   a. Business – Business Reference Model (BRM)
   b. Data – Data Reference Model (DRM)
   c. Application – Service Component Reference Model (SRM)
   d. Technology – Technology Reference Model (TRM)

e-Government / Portal Objective 2: The State will establish a common Internet portal infrastructure

The State, through the Statewide Internet Portal Authority (SIPA), will encourage a World-wide Web based state government utilizing shared technology to include Web hosting, security, and portal services such as search, directory, access, content management, and agency-specific online services.

Actions to Achieve e-Government / Portal Objective 1

1. By April 1, 2006, **OIT** will document and communicate the State governance model, consistent with SIPA's governance model, for agency adoption and migration of portal services as part of the Annual Information Technology Budget and Planning Process.
2. By June 1, 2006, **SIPA** will establish a catalog of Web development / application services available for use by state agencies.
3. By June 1, 2006, **state agencies** will submit to OIT and SIPA a list of applications or services as candidates that can be supported / developed by the portal integrator.

Initiative 3: Common / Shared Services

Common and interoperable systems will provide more robust, comprehensive business capabilities

The State will consolidate its technology infrastructure and services to leverage the economies of scale in the utilization of resources, eliminating unnecessary redundancies, and reducing support cost through standardization. These efforts will align with the development of the enterprise architecture and implement the strategic direction for the use and deployment of information technology solutions statewide.

The State will replace duplicate, conflicting, and outdated applications and systems with common solutions that are interoperable across all State departments. Technology consolidation by the departments will increase the security, robustness, and reliability of the State's technology-enabled business infrastructure as well as improve budget allocation, cross-agency collaboration, e-government solutions, information sharing, and performance management.

Common / Shared Services Objective 1: The State will consolidate e-mail service

The State owns and operates over 200 e-mail servers. e-Mail has evolved into a business commodity that can be easily provided at large scale as a centrally administered service or as an outsourced service. The State will consolidate the management of all e-mail services. The consolidation will reduce the level of effort by agency staff in administering e-mail, reduce the overall e-mail administrative and infrastructure costs to the State, and improve security, reliability and redundancy.

Actions to Achieve Common / Shared Services Objective 1

1. By April 30, 2006, **DoIT (DPA)** will submit an e-mail consolidation plan (including overall approach, scope and budget) to the State CIO and the State Budget Director for final approval.
2. By June 30, 2006, **DoIT (DPA)** will implement a production consolidation sized appropriately to measure key metrics for managing day-to-day operations, establish service level metrics, and key performance indicators.
3. By September 1, 2006, **each agency** will have established its migration plan for subscribing to the centrally administered service based on the results of the department surveys and assessments.

Common / Shared Services Objective 2: The State will reform information technology procurement

Agencies independently acquire uncoordinated and duplicative information resource technologies that are more appropriately acquired as part of a coordinated effort for maximum cost effectiveness and use. The State will aggregate those communication, information resource, and technology procurements that would be beneficial.

Actions to Achieve Common / Shared Services Objective 2

1. By May 1, 2006, the **IMC** and **OIT** will facilitate reviewing and analyzing, in collaboration with state agencies, their information technology procurements planned for the remainder of FY05-06.
2. By June 1, 2006, **OIT** will work with the **State Purchasing Office** to administer an information technology aggregated procurement for multiple state agencies.

Common / Shared Services Objective 3: The State will utilize common data center facilities

Natural disasters and the rise of domestic and international terrorism place the State's technology systems at increased risk at a time when business functions are becoming increasingly dependent on reliable technology support. Catastrophic events, as well as attacks against our technology infrastructure and systems, can have a severe impact on business operations.

We must work together to ensure that all of Colorado's critical (mission essential) systems are sufficiently safeguarded in appropriate facilities by robust recovery plans and assets in order to maintain business continuity of state government.

Actions to Achieve Common / shared Objective 3

1. By December 31, 2006, **OIT**, in partnership with the Division of Emergency Management (Department of Local Affairs), will assist all agencies in drafting Continuity of Operations Plans (COOPs) with complete documentation of information technology disaster recovery capabilities and needs.
2. By June 30, 2007, each **agency** will complete plans for providing robust disaster recovery functionality to all of their critical systems by June 30, 2008.
3. By June 30, 2007, **50% of agencies** with existing disaster recovery assets will have such located at the Statewide Disaster Recovery data center facility opened by CDOS.

Initiative 4: IMC / Governance

Leverage the IMC to mature the Technology Governance Structure for coordinating and directing state agency use of information technology

The IMC was created during the 1987 legislative session with the passage of Senate Bill 98-246. The purposes of the IMC as defined by the legislature and stated in C.R.S. 24-37.5 are as follows:

- Oversee strategic planning and set policy for the state's information systems; and,
- Assure continuity in planning and controlling the state's investment in information systems.

IMC / Governance Objective 1: The state will implement strategic information technology performance management

Organizations are continuously challenged with how to effectively implement an enterprise strategy throughout the organization and monitor that strategy's performance at strategic and tactical levels.

The state must continue to advance its understanding of, and ability to articulate, information technology costs, services and benefits in relevant business terms to clearly demonstrate the value IT provides. This will better position the State to eliminate duplicate systems, successfully replace antiquated, non-supported hardware and software, as well as increase the adoption of enterprise-wide common technology solutions.

Actions to Achieve IMC / Governance Objective 1

1. By March 1, 2006, the **State CIO** and **State Budget Director** will evaluate the need for an enterprise portfolio management software tool.
2. By April 1, 2006, the **IMC** will adopt an information technology asset management standard for the State.
3. By May 1, 2006, the **IMC** and **OIT** will distribute an assessment model illustrating how the 2006 Statewide Information Technology Plan will be used in evaluating and providing recommendations on annual Department IT Plans (DITPs), IT budget requests, IT project proposals, and IT procurements.

IMC / Governance Objective 2: The State will prepare for more rigorous information technology risk management evaluation

The State will refine and expand the current process for monitoring information technology projects, initiatives, and procurement requests to ensure prioritization and alignment to the State's information technology strategic goals as well as the mission and goals of the State agencies. The refined and expanded process will also ensure adequate risk mitigation and controls are in place for large information technology initiatives.

Actions to Achieve IMC / Governance Objective 2

1. By March 1, 2006, the **IMC** will adopt a new Model IT Contract and IT Administrative Guide.
2. By March 31, 2006, **IMC** will adopt the common project management methodology as developed by the statewide Project Management User Group (PMUG).
3. By May 1, 2006, the **IMC** will partner with the Attorney General's Office and State Controller's Office (SCO) to require state agency use of model IT contracts.
4. By August 1, 2006, **IMC/OIT** will establish, document and communicate an enterprise IT Risk Management process that will focus on:
    - Identifying project risk and assessing their potential impact;
    - Establishing effective risk mitigation strategies;
    - Managing and controlling risk throughout the project lifecycle; and
    - Implementing adequate governance for oversight on IT projects
5. By October 1, 2006, **PMUG** establish a mentoring program and project management common methodology training classes.

Conclusion

The 2006 Colorado State Information and Technology Strategic Plan outlined a bold agenda across four initiatives to increase the value delivered to the government and constituents from our information technology investment. These four initiatives each have objectives that can be achieved over the next 12 months and that are the responsibility of one, or a small group, of information technology or public service professionals. The four initiatives are:

Initiative 1: **Cyber-Security** - Improved security of information;

Initiative 2: **e-Government / Portal** - Better integration and access to government services;

Initiative 3: **Common / Shared Services** - Better application of economies of scale and improved use of; and,

Initiative 4: **IMC / Governance** – Further leveraging our information technology governance structure to assure continuity in planning and controlling the state's investment in information technology.

The first three initiatives benefit the government or our constituents directly in the current year i.e., Cyber-Security and e-Government / Portal, as well as in future years. The last, IMC / Governance primarily provides benefits in the next and following years.

Each of the four initiatives supports our agenda to redefine how we manage our information technology resources to improve service delivery and streamline business operations. They uphold the Governor's highest information technology priority commitments while delivering measurable results in the short-term. Each of the four initiatives sit clearly within the OIT's adopted mission i.e., deliver secure services (Cyber-Security); deliver cost-effective, reliable, and accessible services (e-Government / Portal); use information technology to maximize efficient service delivery (Common / Shared Services); and, information technology will operate as a seamless enterprise (IMC / Governance).

Across the four initiatives, those involved in delivering the actions identified within this document are limited to the CISO, Agency CIOs, the IMC, SIPA, DoIT (DPA), the State Budget Director, PMUG, OIT and its Director – the State CIO. Most importantly, almost all of those identified contributed to the writing of the plan and have agreed to the actions and associated due dates. In addition, those identified represent all the state agencies and can act as a focal point for action and responsibility.

Specifically, Cyber-security efforts will establish an environment that provides measurable standards for risk mitigation and offer state agencies the tools necessary to secure their information technology operations. e-Government efforts will adopt an Enterprise Architecture as a means of connecting individual agency goals to a shared information technology strategy thereby helping the enterprise improve the return on its information technology investments.

Through the Statewide Internet Portal Authority, the State will encourage a World-wide Web based state government utilizing shared technology to include Web hosting, security, and portal services such as search, directory, access, content management, and agency specific online services.

Common / Shared Services efforts will consolidate technology infrastructure and services to leverage the economies of scale in the utilization of resources, eliminating unnecessary redundancies, and reducing support cost through standardization.

The IMC / Governance efforts will continue to oversee strategic planning and set policy for the state's information systems, and assure continuity in planning and controlling the state's investment in information systems. A key focus will be to refine and expand the current process for monitoring information technology projects, initiatives, and procurement requests to ensure prioritization and alignment to the State's information technology strategic goals.

Finally, in addition to the current benefits these four initiatives deliver, they form the basis of the next evolutionary step for the State's information technology.

Postscript

As we look ahead at the State's use of information technology to achieve its enterprise goals, we have identified several areas of future interest. The most important of these areas is homeland security.

The strength of our nation's homeland security efforts will continue to leverage information technology infrastructures. Colorado will continue to research, acquire, build, develop, and implement technology solutions that will enhance our efforts in the preparation, prevention, response and recovery of natural or manmade events.

In terms of technology that should be considered for inclusion in our portfolio, mobile technology solutions should continue to be evaluated as an opportunity to enhance our first-responder response and support issues of delivering information technology solutions to rural areas within the state.

We must continue to improve our ability to deliver large, complex information technology solutions on time and on budget. We must also look for integrated solutions where ever we can find them and for services that can be provided directly to citizens and businesses through the Internet or what ever comes after it.

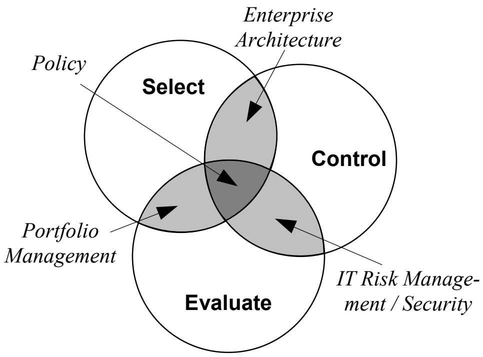
On a broader perspective, we must continue to explore better ways for the many departments within state government to easily collaborate with each other to identify and agree on enterprise solutions to key issues. These key issues will include the ongoing challenge of cyber-security, the next generation common / shared service model, and perhaps the most difficult, an enterprise-level information technology measurement system that supports our focus to deliver value to our constituents.

John Picanso
Chief Information Officer
State of Colorado

Commission on Information Management
225 E 16th Avenue, Suite 260
Denver, Colorado 80203-1606

Phone: 303-866-6060
Fax: 303-866-6454

www.colorado.gov/oit


Enterprise Architecture
Policy
Select
Control
Portfolio Management
Evaluate
IT Risk Management / Security